DECISIONE (PESC) 2020/1748 DEL CONSIGLIO

del 20 novembre 2020

che modifica la decisione (PESC) 2019/797 concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri

IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sull'Unione europea, in particolare l'articolo 29,

vista la proposta dell'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza,

considerando quanto segue:

(1) Il 17 maggio 2019 il Consiglio ha adottato la decisione (PESC) 2019/797 ([1]).

(2) Il 30 luglio 2020 il Consiglio ha adottato la decisione (PESC) 2020/1127 ([2]), con la quale sono state aggiunte sei persone fisiche e tre entità od organismi all'elenco delle persone fisiche e giuridiche, delle entità e degli organismi soggetti a misure restrittive che figura nell'allegato della decisione (PESC) 2019/797.

(3) Sono state ricevute informazioni aggiornate per due voci dell'elenco delle persone fisiche.

(4) È opportuno pertanto modificare di conseguenza la decisione (PESC) 2019/797,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

L'allegato della decisione (PESC) 2019/797 è modificato conformemente all'allegato della presente decisione.

Articolo 2

La presente decisione entra in vigore il giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Fatto a Bruxelles, il 20 novembre 2020

Per il Consiglio
Il presidente
M. ROTH

([1]) Decisione (PESC) 2019/797 del Consiglio, del 17 maggio 2019, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri (GU L 129I del 17.5.2019, pag. 13).

([2]) Decisione (PESC) 2020/1127 del Consiglio, del 30 luglio 2020, che modifica la decisione (PESC) 2019/797, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri (GU L 246 del 30.7.2020, pag. 12).

ALLEGATO

Nell'allegato della decisione (PESC) 2019/797, nella sottorubrica «A. Persone fisiche», le voci 1 e 2 sono sostituite dalle seguenti:

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
«1.	GAO Qiang	Data di nascita: 4 ottobre 1983 Luogo di nascita: Shandong Province, Cina Indirizzo: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, Cina Cittadinanza: cinese Sesso: maschile	Gao Qiang è coinvolto nella campagna «Operation Cloud Hopper», una serie di attacchi informatici con effetti significativi che proviene dall'esterno dell'Unione e costituisce una minaccia esterna per l'Unione o i suoi Stati membri e di attacchi informatici con effetti significativi nei confronti di Stati terzi. La campagna «Operation Cloud Hopper» ha preso di mira i sistemi di informazione di imprese multinazionali in sei continenti, tra cui imprese situate nell'Unione, e ha ottenuto l'accesso non autorizzato a dati sensibili sotto il profilo commerciale, causando perdite economiche significative. Il soggetto noto pubblicamente come «APT10» («Advanced Persistent Threat 10») (alias «Red Apollo», «CVNX», «Stone Panda», «MenuPass» e «Potassium») ha condotto la campagna «Operation Cloud Hopper». Gao Qiang può essere collegato all'APT10, anche attraverso la sua associazione con l'infrastruttura di comando e controllo di APT10. Inoltre, Huaying Haitai, un'entità designata per il fatto di fornire sostegno e agevolare la campagna «Operation Cloud Hopper», ha impiegato Gao Qiang. Quest'ultimo ha legami con Zhang Shilong, la cui designazione è altresì connessa alla campagna «Operation Cloud Hopper». Gao Qiang è pertanto associato sia a Huaying Haitai che a Zhang Shilong.	30.7.2020
2.	ZHANG Shilong	Data di nascita: 10 settembre 1981 Luogo di nascita: Cina Indirizzo: Hedong, Yuyang Road No 121, Tianjin, Cina Cittadinanza: cinese Sesso: maschile	Zhang Shilong è coinvolto nella campagna «Operation Cloud Hopper», una serie di attacchi informatici con effetti significativi che proviene dall'esterno dell'Unione e costituisce una minaccia esterna per l'Unione o i suoi Stati membri e di attacchi informatici con effetti significativi nei confronti di Stati terzi. La campagna «Operation Cloud Hopper» ha preso di mira i sistemi di informazione di imprese multinazionali in sei continenti, tra cui imprese situate nell'Unione, e ha ottenuto l'accesso non autorizzato a dati sensibili sotto il profilo commerciale, causando perdite economiche significative. Il soggetto noto pubblicamente come «APT10» («Advanced Persistent Threat 10») (alias «Red Apollo», «CVNX», «Stone Panda», «MenuPass» e «Potassium») ha condotto la campagna «Operation Cloud Hopper». Zhang Shilong può essere collegato all'APT10, anche attraverso il malware che ha sviluppato e testato in relazione agli attacchi informatici condotti dall'APT10. Inoltre, Huaying Haitai, un'entità designata per il fatto di fornire sostegno e agevolare la campagna «Operation Cloud Hopper», ha impiegato Zhang Shilong. Quest'ultimo ha legami con Gao Qiang, la cui designazione è altresì connessa alla campagna «Operation Cloud Hopper». Zhang Shilong è pertanto associato sia a Huaying Haitai che a Gao Qiang.	30.7.2020».